Unified Capabilities Approved Products List (UC APL) Security Technical Implementation Guide (STIG) Applicability Questionnaire

For Developers and Vendors

Version 4, Release 0

January 2014

Developed by DISA for the DoD

1. INTRODUCTION

Per the Unified Capabilities (UC) Approved Product List (APL) Process Guide, the vendor is required to complete the Security Technical Implementation Guide (STIG) Questionnaire. All products or systems on a Department of Defense (DoD) network is required to be secured in accordance with the applicable DoD STIGs. To use this questionnaire, answer the questions below by checking the boxes. Each checked box indicates one or more required STIGs, checklists or tools. Please refer to the Information Assurance Support Environment website for a list of all of the STIGS, Checklists, Security Requirements (SRG), Security Content Automation Protocol (SCAP) Benchmarks, and Security Readiness Review Evaluation Scripts (SRR).

http://iase.disa.mil/
http://iase.disa.mil/stigs/index.html

The SRRs and SCAP Tools must be requested from your Sponsor

An engineer who is fully knowledgeable of the system to be tested must complete this technical questionnaire. This engineer should be the one who will participate in or will directly support the testing effort.

Name of the Product or System: ______________________________

Model of the Product or System: ______________________________

Version and patch level of the Product or System: ______________________

Firmware/Kernel: ______________________________

□ First time in the UC Process □ Product currently on APL – this is an update

HAS THE PRODUCT BEEN TESTED BY ANY US GOVERNMENT OR DEPARTMENT OF DEFENSE (DOD) ENTITY?

____
Purpose for the test

____
Name and location (if known) of the entity conducting the test

____
The dates (rough estimate is okay) testing occurred

List each component - defined as a single device or box that has a single instance of an operating system. (if you need more space, please print this page and add the additional devices)

1. Functional name of the device: ____

Function performed: ____

2. Functional name of the device: ____

Function performed: ____

3. Functional name of the device: ____

Function performed: ____

4. Functional name of the device: ____

Function performed: ____

5. Functional name of the device: ____

Function performed: ____

6. Functional name of the device: ____

Function performed: ____

7. Functional name of the device: ____

Function performed: ____

8. Functional name of the device: ____

Function performed: ____

2. SOLUTION OR SYSTEM GENERAL TYPE AND/OR FUNCTION

UC General Device Type

Voice, Video, and Data Services

□ Classified Voice
□ Classified Video
□ Data
□ SBU Voice
□ SBU Video
□ Multi Function Mobile Devices

Network Infrastructure

□ Transport
□ Routers/Switches
□ Security
□ Enterprise Network Management
□ Storage

Functions

Check all that applies:

□ AGS
□ OTS
□ FNE
□ DNE
□ Access Aggregate Function M13

□ Aggregation Router
□ Provider Edge Router
□ Customer Edge Router
□ Access IP Switch
□ Distribution IP Switch
□ Core IP Switch
□ Wireless LAN

□ EBC
□ Data Firewall
□ WIDS
□ IDS/IPS
□ VPN
□ HAIPE
□ Link Encryptors
□ Integrated Security Solution
□ Network Access Control

□ EMS
□ Operation Support System

□ Data Storage Controller

□ WAN Soft Switch
□ LSC
□ Dual Signaling Soft Switch
□ AS-SIP End Instrument
□ AS-SIP to TDM GW
□ AS-SIP to IP GW
□ Multi Signaling Conference Bridge

□ WAN Soft Switch
□ ESC
□ MFSS
□ RTS Routing Database
□ Multi Signaling MCU
□ RTS Statefull FW

□ Mobile Devices

□ An Application

Solution Management

□ The management application includes a vendor application and coding. The **Application Security and Development STIG** is applicable.
□ No separate management application – built into the network device

The solution is managed – Check all that apply:
□ From a client via HTTPS
□ Installed executable locally on server
□ Installed executable on a client
□ Locally via a directly connected external terminal or emulator
Specify Interfaces and Technology(s): ___________________
□ Remotely across a Network______________
Specify Interfaces and Technology(s): ___________________
□ Remotely via Dialup______________

IA/Encryption

□ Encryption is used. Type_________________________________

□ The encryption module or software tool kit is FIPS 140-2 validated.

□ The encryption is NSA type 1 certification.

____

Listing of the encryption module(s)/algorithm(s) used

____

Encryption module(s) vendor(s)

____

Certification number(s)

____

Validation level(s)

□ If IA or IA-Enabled product, the product is Common Criteria or NIST certified (submit certificated)

□ If IA or IA-Enabled product, the product is in the process of seeking Common Criteria or NIST certification (submit letter with status or acceptance in the process)

Name of the Common Criteria Testing Laboratory (CCTL)

____

Protection Profile (PP)

____

Evaluation Assurance Level (EAL)

____

Evaluation Report Number

____

Date of Issuance

□ The product use PKI or X.509 type certificates.

□ The system is DoD PKI enabled or compatible.

□ The system supports DoD Common Access Card

3. NETWORK

□ IPV6 is supported

Backbone Transport STIG/Checklists: (check all that applies)

□ Optical Transport □ DWDM NE □ Router

□ SONET NE □ ODXC □ MPLS

□ MSPP NE □ Backbone/Core □ Internet Access Points

Router Checklists: (check all that applies)

□ Cisco □ Juniper □ Router SRG

Network Infrastructure Checklists: (check all that applies)

□ Firewall

□ Intrusion Detection System / Intrusion Protection System

□ Router Layer 3 Switch

□ Layer 2 Switch

□ Other Device

□ Perimeter Router Layer 3 Swich

□ Network Policy

□ Network SRG

□ Other – Please Specify with version: ____________________________________

4. OPERATING SYSTEM

Windows Operating System, check the applicable checklist and benchmark:

□ Windows 2000 Server - □ Stand Alone/Member □ Domain Controller

□ Windows 2003 Server - □ Stand Alone/Member □ Domain Controller

□ Windows 2008 Server - □ Stand Alone/Member □ Domain Controller □ R2

□ Windows 7 Professional

□ Windows 8 Professional

□ Windows XP Professional - □ Embedded

□ Windows 2000 Professional - □ Embedded

□ Windows Vista

□ Operating System Security Requirements Guide

UNIX flavor Operating System, check the applicable checklist and benchmark:

□ SUN Solaris - □ 9 □ 10 AND □ SPARC □ X86

□ Red Hat - □ 5 □ 6

□ HPUX - □ 11.23 □ 11.31

□ AIX - □ 5.3 □ 6.1

The **UNIX Security Requirements Guide (SRG)** is applicable to all other flavors not listed above

□ Other – Please Specify with version: ___________________________________
(ie VxWorks,)

□ The UNIX or Linux is embedded
Note: The STIGs is not applied if the OS is embedded and there is no access to a command line from any interface to make OS configuration changes.

Mac Operating System, check the applicable checklist and benchmark:

□ 10.5 □ 10.6

5. SOFTWARE AND APPLICATIONS

Web Server and/or Application Services STIG, check the applicable checklist.

□ Apache 2.0
□ Apache 2.2
□ IIS 6
□ IIS 7
□ IIS 6

□ Other – Please Specify: ______________________________

The application uses a HTTP browser or mobile code such as Internet Explorer or Mozilla (or other) to access any portion of its functionality or management.

□ Web browser SRG
□ Mozilla Firefox SRG
□ Web Policy Manual STIG

If application uses mobile code.
Please Specify: _____________________________________

Supported	Required	Test with	
□	□	□	Firefox
□	□	□	IE v6
□	□	□	IE v7
□	□	□	IE v8
□	□	□	IE v9
□	□	□	IE v10
□	□	□	Other: Please Specify - _______________

The system supports antispyware and Commercial-Off-The-Shelf Products (MS Office)
Select the applicable checklists.

□ MS Office 2003
□ MS Office 2007
□ MS Office 2010

□ The Desktop Application STIG is applicable.
□ Other – Please Specify: ________________________________

The system store information (such as configuration information) in tables or use a file structure that would typically be known as a database. Determine the **Database STIG** indicating the applicable checklist and SRR scripts below:

□ Oracle 9i □ Oracle 10g □ Oracle 11g
□ SQL Server 2000 □ SQL Server 2005 □ SQL Server 7
□ MS-SQL

□ The database a back-end-to the application with no user access?

The **Database Security Requirements Guide (SRG)** is applicable to all other databases not listed above
□ Other – Please specify with version: _____________________________________
(MySQL, Access,)

Determine if the **Application Services STIG** is applicable by selecting the below checklists:

□ Tomcat
□ Weblogic
□ Sun Java
□ JVM J2SE
□ Application Server

The system uses **.NET Framework**. Check the applicable checklist
□ MS .NET Framework 4 and benchmark
□ .NET Framework Security for versions 1.0, 2.1, 2.0, 3.0, and 3.5

Note: See the NSA Guide to Microsoft .NET Framework Security,

The system contains a **Domain Name Services (DNS)** server

□ DNS SRG is applicable.
Please Specify: _______________________________________

The system is an **Access Control Solution**.

□ The Access Control STIG is applicable.

6. MOBILE DEVICES

The system is a **mobile device**, check the applicable checklist:

□ Android 2.2
□ Blackberry
□ Apple IOS 6
□ Samsung Knox Android 1.0
□ Mobile Application SRG
□ Mobile OS SRG
□ Mobile Policy SRG
□ Other:_______________________________________

7. OTHER FEATURES AND CAPABILITIES OF THE SYSTEM

The below exists within the system:

□ Citrix XenAPP

The system supports telecommunications traffic in the form of voice, video, data (via modem) or fax.

□ The Defense Switch Network is applicable.
□ The Secure telecommunications and DRSN is applicable.

The system uses Virtual Network, check the applicable checklist.

□ ESXi5 Server
□ ESXi5 Virtual machine
□ Virtual machine checklist

The system is a MS Exchange Server

□ MS Exchange 2003
□ MS Exchange 2010

The system is a network level Firewall., not a host-based firewall.

□ Firewall SRG

The system is an Intrusion Detection System / Intrusion Protection System

□ Intrusion Detection and Prevention System SRG

The system is an IPSEC VPN
□ IPSEC VPN Gateway STIG

The system is a Keyboard Video and Mouse (KVM) solution.
□ The Access Control STIG is applicable.

The system is a Multifunction Devices (MFD) and Printer solution.
□ The MFD and Network Printers STIG

The system supports remote access and/or management.
□ Remote Access Policy STIG
□ Remote Access Server STIG
□ Remote Access VPN STIG
□ Remote Endpoint SITG
□ Remote XenAPP ICA Think Client
□ Remote Storage STIG

The system supports VoIP technology.
□ Voice and Video over Internet Protocol
□ Remote Access Server STIG

The system supports Wireless technology.
□ Wireless STIG

8. PROTOCOLS

Check off all of the following protocols that are used by the system/device:

□ FTP
□ TFTP
□ BootP
□ RCPl
□ SSH Version _____
□ SFTP
□ SNMP Version ____
□ SSL Version ______

□ TLS
□ IPSEC
□ h.323
□ h.320
□ SIP
□ SMTP

□ SIP-TLS
□ AS-SIP
□ RTP
□ SRTP
□ LDAP

□ Proprietary Signaling Protocol – Detail: ____________________
□ Proprietary Bearer Protocol – Detail: ______________________
□ Other – Please Specify: __________________________________